電子メール利用ガイドライン

関西大学 IT センター

1　本ガイドラインの目的

電子メールは日々の学習・教育・研究活動において必要不可欠なものになっている。そのため、電子メールは、ルールやマナーを守った安全な方法で使用しなければ、多くの利用者に迷惑をかけることになる。その上、誤った方法による使用は学習・教育・研究活動の停止や社会的信用を失わせる要因となる可能性もある。本ガイドラインは、このようなリスクを軽減し、情報資産を保護し、電子メールを安全に利用するための手順を提供する。

2　本ガイドラインの対象者

本ガイドラインは、IT センターが整備・提供する電子メールを利用するすべての利用者を対象とする。

3　電子メールソフトの設定

⑴ 電子メール受信に係る設定

ア　利用者は、受信した電子メールをテキスト（リッチテキストを含む）として表示することを推奨し、偽のホームページへの誘導や不正なスクリプト（プログラム）の実行を未然に防ぐ目的から HTML メールはできる限り利用しないことを推奨する。

イ　利用者は、HTML メールを利用する場合は、HTML メールのプレビュー機能を停止することを推奨する。

ウ　利用者は、アンチウイルスソフトウェアに加えて、電子メールソフトウェア側においてもウイルス対策が設定可能であれば、これを実施する。

⑵ 電子メール送信に係る設定

ア　利用者は、原則として、HTML 形式の電子メールを送信しないことを推奨する。これは、当方より HTML 形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがある。

4　電子メールに係る全般的な注意事項

⑴ 電子メールの私的利用の禁止

ア　利用者は、電子メールシステムを、学習・教育・研究活動を遂行する上で必要な場合のみ使用することとし、私的目的のために使用しない。

⑵ 電子メールを IT センターのアドレス（大学は、@kansai-u.ac.jp）以外に自動転送する場合

ア　利用者は、電子メールを IT センターのアドレス以外に自動転送する場合には、その必要性を十分考慮するとともに、やむをえない場合は、転送先アドレスが間違っていないこと、転送先で機密性が保たれることを確認する。特に転送先のアドレスを変更または停止した場合、直ちに自動転送の設定を修正する。

⑶ 電子メールの監視

ア　電子メールシステムの適正な利用のため、その利用状況（あて先、内容、添付ファイル等）について証跡の取得、保存、点検及び分析が行われる可能性がある。利用者は、その趣旨を理解の上、電子メールの内容に関するモニタリング及び監査を実施していることを認識する。

⑷ 電子メール ID 及び電子メールアドレスの管理

ア　利用者は、他人の電子メール ID （電子メールサーバへのログイン ID。以下同じ。） 及び電子メールア

ドレスを使用しない。

イ　利用者は、電子メール ID 及び電子メールアドレスを他人と共用しない。

ウ　利用者は、自己に付与された電子メール ID を、それを知る必要のない者に知られるような状態で放置しない。

エ　特定のサービス、職位、部門単位に付与されるメーリングリストのように、電子メールアドレスを複数の関係者で共用するあるいは担当者が引き継いで使用する必要がある場合には、利用者はその許可及び設定について IT センターに相談する。

5　パスワードの管理

(1) 電子メールパスワードの管理

ア　利用者は、パスワードを設定する。

イ　利用者は、パスワードの管理にあたっては「パスワード利用ガイドライン」に従う。

ウ　利用者は、パスワードを電子メールソフトに永続的に保存しない。ただし、電子メールの受信のたびにパスワード入力を行うことが過度に煩雑である場合には、電子メールソフトに一時保存し、クライアント PC 及びスマートフォン等の携帯情報端末起動後のみパスワード入力とする仕組みを利用してもよい。

エ　利用者は、パスワードを電子メールソフトに一時保存する場合には、当該パスワードを一時保存するクライアント PC 及びスマートフォン等の携帯情報端末を「主体認証情報格納装置」とみなして、以下の点に配慮して安全に取り扱う。

（ア）　パスワードを保存したクライアント PC 及びスマートフォン等の携帯情報端末を本人が意図せずに使用されることのないように安全措置を講じる。

（イ）　パスワードを保存したクライアント PC 及びスマートフォン等の携帯情報端末を他者に付与及び貸与しない。

（ウ）　パスワードを保存したクライアント PC 及びスマートフォン等の携帯情報端末を紛失しないように管理する。紛失した場合には、直ちに IT センターにその旨を報告する。

6　電子メールの受信

(1) 電子メールの受信確認

ア　利用者は、定期的に、電子メールの受信確認を行う。

(2) 電子メール添付ファイルのウイルスチェック

ア　利用者は、アンチウイルスソフトウェアによる自動ウイルスチェックを実施する。

イ　利用者は、自動的にウイルスチェックを実施するように設定している場合または自動的にウイルスチェック最新データを更新するように設定している場合は、当該設定を変更しない。

ウ　利用者は、受信した電子メールの添付ファイルに対して、随時、ウイルスチェックを行う。これは、新種のウイルスに対応したパターンファイルの提供が間に合わず、ファイル受信時のウイルスチェックにおいてウイルスが発見されなかった場合を考慮し、最新のパターンファイルを用いて過去に受信した電子メールの添付ファイルに対してもウイルスの有無を確認するための対策である。

エ　利用者は、緊急時対応が必要なときには、IT センターからの指示に従う。

(3) あて先間違いの電子メールを受信したときの対処

ア　利用者は、あて先間違いの電子メールを受信し、送信者から正しい受信者へ再度送信する必要がある場合には、可能な範囲で送信者へあて先が間違っていたことを通知する。

イ　利用者は、あて先間違いの電子メールを受信した場合には、これを削除する。

⑷ 不審な電子メールを受信したときの対処

ア　利用者は、不審な電子メールを受信した場合には、電子メールを開かず、IT センターに連絡・相談し、指示を仰ぐ。

イ　利用者は、電子メールに不審なファイルが添付されていた場合には、当該ファイルを開くことなくITセンターに連絡・相談し、指示を仰ぐ。

⑸ ウイルスに感染したときの対処

ア　利用者は、クライアント PC 及びスマートフォン等の携帯情報端末がウイルスに感染した場合または感染したと疑われる場合には、更なる感染を未然に防止するため、「直ちに」当クライアント PC 及びスマートフォン等の携帯情報端末をネットワークから分離し、IT センターに連絡・相談し、指示を仰ぐ。ネットワークからの分離は、具体的には、PC の場合はネットワークケーブル、無線 LAN カード、USB キー型無線 LAN アダプタなどを取り外す。または、無線 LAN アダプタが PC に内蔵されている場合には無線 LAN 機能を停止させる。携帯情報端末の場合は機内モードをオンにする、または Wi-Fi と 4G などの無線通信をオフにする。

⑹ 迷惑メールの対処

ア　利用者は、必要以上に電子メールアドレスを公表または通知しない。

イ　利用者は、ホームページ等でネットワークを経由して電子メールアドレスを開示または通知する場合には、アドレスを自動収集されないように、工夫を施すことが望ましい。

（ア）　アドレスを画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等。

ウ　利用者は、送信される迷惑メールに対しては、これを無視する。送信者へ停止要求を出した場合、その電子メールアドレスが使用されている事実を伝えてしまう結果となり、かえって迷惑メールが増加してしまう可能性がある。

7　電子メールの作成

⑴ To、Cc 及び Bcc の制限

ア　利用者は、To（あて先）、Cc（カーボンコピー）及び Bcc（ブラインドカーボンコピー）の総あて先件数は必要最低限とする。

（ア）　使用するネットワークリソースが、電子メール１件の使用リソース×総あて先件数となる。

イ　利用者は、同時に多数の人へ電子メールを送信する場合、Bccを利用するかあるいは各自に個別送信する等配慮する。これは、その場合に電子メールアドレスをTo、Ccに列記してしまうと、当該電子メールを受信した者に、他の者の電子メールアドレスが露呈することになる。

⑵ 電子メール１件当たりのファイル容量の制限

ア　利用者は、電子メール本体と添付するファイルを含めた総容量が 25MByte を超えないようにする。

（ア）　IT センターが提供する電子メールシステムでは、送信の際の容量制限を 25MByte としている。

イ　利用者は、電子メール本体と添付するファイルを含めた総容量が25MByteを超える場合、関大ファイル

便（容量制限は、１GByte）等の別手段による情報提供や分割送信などについて検討する。

⑶ 電子メールの形式の制限

ア　利用者は、できる限り、HTML 形式の電子メールを送信しない。これは、当方より HTML 形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがある。

⑷ 電子メールの内容

ア　利用者は、要機密情報を電子メールで送信する場合は別途定められた安全措置を講ずる。

（ア）　利用者は、要機密情報を電子メールで送信する場合には、適宜、上司に届け出、許可を得る。

（イ）　利用者は、要機密情報を電子メールで送信する場合には、安全確保に留意して送信手段を決定する。例えば以下の手段が挙げられる。

a　関大ファイル便

b　インフォメーションシステムの個人伝言

c　暗号化された通信路（VPN 等）

d　外部を経由しないネットワーク（専用線等）

（ウ）　利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、以下の保護対策の必要性を検討し、必要があると認めたときには、これを実施する。

a　添付ファイルに対するパスワード保護

b　添付ファイルの暗号化（暗号化ソフトの使用等）

イ　利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与する。

ウ　利用者は、電子署名の付与に用いた鍵を適切に管理する。

エ　利用者は、他人になりすまして電子メールを作成しない。

オ　利用者は、電子メールを転送する際に、作成者の許可なく内容の変更をしない。

カ　利用者は、個人情報やプライバシーの保護を考慮する。

キ　利用者は、次の事項に該当する電子メールの送信を行わない。

（ア）　機密保護違反（『学校法人関西大学文書取扱規程』『学校法人関西大学情報システム利用規程』を遵守する）

（イ）　権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）

（ウ）　セクシャルハラスメント及び人種問題に関わる内容

（エ）　無礼及び誹謗中傷

（オ）　ねずみ講に相当する内容

（カ）　脅迫、個人的な儲け話や勧誘に相当する内容

⑸ ネチケット

ア　利用者は、チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わない。

イ　利用者は、スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール）、

ジャンクメール（役に立たない情報が書かれている電子メール）等を送信しない。

ウ　利用者は、電子メールに件名（Subject）を付ける。また、件名は電子メールの内容が分かるように具体的かつ簡潔に書く。

エ　利用者は、俗語的表現やあらかじめ定められていない省略語を使用しない。

オ　利用者は、機種依存文字コードを使用しない。

（ア）　利用者が判断できない場合には、ITセンターに相談し、指示を仰ぐ。

カ　利用者は、電子メールを作成する際、各行とも全角30～35文字程度を目安に、適宜改行を入れる。

キ　利用者は、ToとCcとの使い分けを意識し、送信する電子メールに対する返事を要求するときには、To（あて先）を使用する。

8　電子メールの送信

⑴ 送信時の注意

ア　利用者は、To（あて先）の記述に誤りがないかを確認してから送信する。

イ　利用者は、電子メールにファイルを添付し送信する際に、当該ファイルのウイルスチェックを行う。

⑵ 電子メールの暗号化

ア　利用者は、要機密情報を電子メールで送信する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化する。

（ア）　通信路の暗号化（関大ファイル便、インフォメーションシステムの個人伝言等）

（イ）　添付ファイルの暗号化（暗号化ソフトの使用等）

イ　利用者は、暗号化された情報の復号に用いる鍵を適切に管理する。

ウ　利用者は、暗号化された情報の復号に用いる鍵のバックアップを取得しておく。

⑶ 添付ファイルのパスワード保護

ア　利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、添付ファイルにパスワードを設定する。

[操作手順]　文書ファイルのパスワードのかけ方（Word の場合）
Word の[ファイル]メニューから[名前を付けて保存]を選択した後、[ツール]から[全般オプション]を選択し、[読み取りパスワード]を設定する。

イ　利用者は、保護に用いたパスワードについては、あらかじめ受信者と合意した文字列を用いるかあるいは電子メールで送信せずに電話などの別手段を用いて伝達する。

⑷ 電子メール送信時における情報漏えい防止の確認事項

ア　利用者は、添付ファイルを電子メールで送信する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないか確認する。

（ア）　「プロパティ」に作成者や修正者等の個人情報が残っていないか

（イ）　一見すると表示されていない部分（「非表示」の設定箇所、非表示としたコメント、裏に隠れたシー

ト等）に要機密情報が含まれていないか

（ウ） 変更履歴が必要以上に保存されていないか

⑸ 電子メールへの署名付与

ア 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与する。

イ 利用者は、電子署名の付与に用いた鍵を適切に管理する。

⑹ 電子メール送信時の受信確認機能の使用制限

ア 利用者は、トラフィック増を防止するため、電子メール送信時の受信確認は必要最低限の使用とする。

⑺ 電子メールを誤って送信したときの対処

ア 利用者は、電子メールを誤って送信した場合、相手先（受信者）へのフォローは発信者責任で実施する。

⑻ ウイルスを送信したときの対処

ア 利用者は、誤ってウイルスを送信したことが判明した場合、直ちに IT センターに連絡・相談し、指示を仰ぐ。

9 電子メールの保存・削除

⑴ メールボックス（サーバ側）における電子メールの保存・削除

ア 利用者は、サーバの個人別メールボックスに格納される電子メールの最大容量を考慮の上、適宜、メールボックスから不要な電子メールを削除する。

⑵ メールボックス（クライアント PC 及びスマートフォン等の携帯情報端末側）における電子メールの保存・削除

ア 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを保存する場合には、暗号化等の措置を講じた上で保存することが望ましい。

イ 利用者は、本文や添付ファイルに要保全情報が含まれている電子メールについては、適宜バックアップする。

ウ 利用者は、不要なメッセージは速やかにクライアントPC及びスマートフォン等の携帯情報端末から削除する。

エ 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを削除する場合には、その機密性に配慮し、復元が困難な状態にする。

10 本手順に関する相談窓口

⑴ メールボックス（サーバ側）における電子メールの保存・削除

ア 利用者は、緊急時の対応及び本ガイドラインの内容を超えた対応が必要とされる場合には、ITセンターに相談し、指示を受ける。

イ 利用者は、本ガイドラインの内容について不明な点及び質問がある場合には、ITセンターに連絡し、回答を得る。

附 則

1 このガイドラインは、2019年11月６日から施行する。